



# PARKWOOD SECONDARY COLLEGE

## CYBERSAFETY INITIATIVES, CYBER SAFETY PROTOCOLS AND ACCEPTABLE USE AGREEMENT

Cybersafety initiatives and ICT protocols in the college

### Instructions for secondary students:

1. You and your parent/legal guardian/caregiver are asked to read this document
2. If help is needed to understand all the language, or there are any points your family would like to discuss with the College, let the College office know as soon as possible.
3. You and your parent/legal guardian/caregiver should then sign the Student Use Agreement Form return that page to the College.
4. It is important to keep this document for you and your family to read again in the future.

### Important terms used in this document:

- (a) The abbreviation '**ICT**' in this document refers to the term 'Information and Communication Technologies'.
- (b) '**Cybersafety**' refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.
- (c) '**College ICT**' refers to the College's computer network, Internet access facilities, computers, and other College ICT equipment/devices as outlined in (d) below. This also includes subsidiary or public organisation(s) equipment which may extend and/or be part of the college network infrastructure.
- (d) The term '**ICT equipment/devices**' used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs, ipads), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies as they come into use.

## IMPORTANT PARKWOOD SECONDARY COLLEGE CYBERSAFETY INITIATIVES

Parkwood aims to support and actively promote the wellbeing of all students and aims to prevent students becoming 'at risk' of not achieving their academic, social and emotional potential. Our College values respect, fairness, kindness, honesty, trust and tolerance of diversity. These values underpin the strong belief that all students at Parkwood want to learn and do their best. In explicitly teaching these core values, we expect students and teachers to support our six College Norms:

- Follow teachers' instructions
- Allow students and teachers to work without distraction or interruption
- Show respect and tolerance towards other people and property
- Do the set work to the best of their ability
- Be on time for class with the correct books and equipment
- Use ICT responsibly

The measures and protocols outlined in this document are based on these core values and shared expectations and aimed at supporting the college Student Engagement and Wellbeing Policy ([http://www.parkwood.vic.edu.au/image/asp1/Student\\_Engagement\\_and\\_Well\\_Being\\_Policy.pdf](http://www.parkwood.vic.edu.au/image/asp1/Student_Engagement_and_Well_Being_Policy.pdf))

The College's computer network, the Ultranet, Internet access facilities, computers and other College ICT equipment/devices, such as student laptops, bring great benefits to the teaching and learning programmes at Parkwood Secondary College, and to the effective operation of the College. However, it is essential that the College endeavours to ensure the safe use of ICT within the College community.

Thus Parkwood Secondary College has rigorous cybersafety practices in place, which include cybersafety use agreements for all College staff and students.

Cybersafety use agreement documents include information about obligations, responsibilities, and the nature of possible consequences associated with breaches of the use agreement which undermine the safety of the College environment. The cybersafety education supplied by the College to its learning community is designed to complement and support the use of this agreement. The overall goal of the College in this matter is to create and maintain a cybersafety culture which is in keeping with the values of the College, and legislative and professional obligations. All members of the College community benefit from being party to the use agreement and other aspects of the College cybersafety programme.

## **1. Cybersafety use agreements**

- 1.1. All staff and students, whether or not they make use of the College's computer network, Internet access facilities, computers and other ICT equipment/devices in the College environment, will be issued with a user agreement. They are required to read these pages carefully, and return the signed user agreement form to the College office for filing. A copy of this signed form will be provided to the user.
- 1.2. Staff and students are asked to keep the other pages of the agreement for later reference. (If necessary, a replacement copy will be supplied by the College). A copy of the agreement will be kept at the college website.
- 1.3. The College encourages anyone with a query about the agreement to contact the ICT Team as soon as possible.

## **2. Requirements regarding appropriate use of ICT in the College learning environment**

In order to meet the College's legislative obligation to maintain a safe physical and emotional learning environment, and be consistent with the values of the College:

- 2.1. The use of the College's computer network, Internet access facilities, computers and other College ICT equipment/devices, including but not limited student laptops, on or off the College site, is limited to educational purposes appropriate to the College environment. This applies whether or not the ICT equipment is owned/leased either partially or wholly by the College. If any other use is permitted, the user(s) will be informed by the College.
- 2.2. The College has the right to monitor, access, and review all the use detailed in 2.1. The College will use remote access software to ensure appropriate use of ICT devices and the College network. This includes personal emails sent and received on the College's computers and/or network facilities, either during or outside College hours.
- 2.3. The use of any privately-owned/leased ICT equipment/devices on the College site, or at any College-related activity must be appropriate to the College environment. This includes any images or material present/stored on privately-owned/leased ICT equipment/devices brought onto the College site, or to any College-related activity.

Such equipment/devices could include a laptop, desktop, PDA, mobile phone, camera, recording device, ipod, ipad or portable storage (like a USB or flash memory device). Anyone unsure about whether or not it is appropriate to have a particular device at College or at a College-related activity, or unsure about whether the planned use of a particular device is appropriate, should check with the ICT Team.

Note that examples of a 'College-related activity' include, but are not limited to, a field trip, camp, sporting or cultural event, wherever its location.
--

- 2.4. When using a global information system such as the Internet, it may not always be possible for the College to filter or screen all material. This may include material which is inappropriate in the College environment (such as 'legal' pornography), dangerous (such as sites for the sale of weapons), or illegal.

However, the expectation is that each individual will make responsible use of such systems. In the event of their use, students must be able to demonstrate their connection to current classroom learning

### **3. Monitoring by the College**

- 3.1. Parkwood Secondary College has an electronic access monitoring system which has the capability to record Internet use, including the user details, time, date, sites visited, and from which computer or device the http traffic was viewed. The ICT Team also has the ability to remotely monitor College ICT equipment, via logs and real-time screen viewing, including student laptops. You must not attempt to prevent the ICT Team from remotely monitoring any ICT equipment/device
- 3.2. The College monitors traffic and material sent and received using the College's ICT infrastructures. This will be examined and analysed to help maintain a cybersafe College environment.
- 3.3. The College will deploy filtering and/or monitoring software where appropriate to restrict access to certain sites and data, including email.
- 3.4. The College holds the right to access/redirect/stop/copy for evidence of any type of electronic data and remove inappropriate electronic data without notice.
- 3.5. The college holds the right to lock/disable/remove/modify domain/local computer accounts in the event of a threat to the College ICT. This includes any electronic devices which are on the premises of the College.

However, as noted in 2.4, the expectation is that each individual will be responsible in their use of ICT.

### **4. Ownership**

- 1.1 Laptops/ICT equipment remain the property of the College and remain so until the conclusion of the three years. In the event that the student leaves the College before the conclusion of the period of the agreement, the student must return the laptop/ICT equipment.
- 1.2 The College reserves the right to confiscate any laptops/ICT equipment due to breaches of this agreement.

### **5. Audits**

- 5.1. The College will from time to time conduct an internal audit of its computer network, Internet access facilities, computers and other College ICT equipment/devices, or may commission an independent audit. If deemed necessary, auditing of the College computer system will include any stored content, and all aspects of its use, including email. An audit may also include any laptops provided or subsidised by/through the College or subsidised by a College-related source such as the Department of Education and Early Childhood Development.

### **6. Breaches of the use agreement**

- 6.1. Breaches of the use agreement can undermine the values of the College and the safety of the learning environment, especially when ICT is used to facilitate misconduct.
- 6.2. Such a breach which is deemed harmful to the safety of the College such as involvement with inappropriate or illegal material, anti-social activities such as harassment and bullying and possession of Peer-to-Peer software such as Limewire or BitTorrent will constitute a significant breach of discipline and result in serious consequences. A breach of this agreement will result in the laptop or ICT device being reimaged. Any further breaches of this nature will result in changes to the management of the laptop or ICT device. The ICT leader and/sub school coordinator will respond and take appropriate action regarding consequences of all breaches.
- 6.3. If there is a suspected breach of use agreement involving privately-owned ICT on the College site or at a College-related activity, the matter may be investigated by the College. The College may request permission to audit that equipment/device(s) as part of its investigation into the alleged incident.

- 6.4. Involvement with material which is deemed ‘age-restricted’, or ‘objectionable’ (illegal) is a very serious matter, as is involvement in an activity which might constitute criminal misconduct, such as harassment. In such situations, it may be necessary to involve law enforcement in addition to any disciplinary response made by the College as a result of its investigation.

## **7. Other aspects of the College’s cybersafety programme**

- 7.1. The Cybersafety and Acceptable Use agreement operates in conjunction with other cybersafety initiatives, such as cybersafety education supplied to the College community. This education plays a significant role in the College’s overall cybersafety programme, and also helps keep children, young people and adults cybersafe in all areas of their lives. If more information is required, the ICT Team can be contacted.

# PARKWOOD SECONDARY COLLEGE ICT & CYBERSAFETY RULES

These rules have been developed to support the 'Important Parkwood Secondary College Cybersafety Initiative's outlined in Section A and are aimed to further support the college Student Engagement and Wellbeing Policy ([http://www.parkwood.vic.edu.au/image/asp1/Student\\_Engagement\\_and\\_Well\\_Being\\_Policy.pdf](http://www.parkwood.vic.edu.au/image/asp1/Student_Engagement_and_Well_Being_Policy.pdf))

## 1. Staff and students are required to sign use agreements with the College

## 2. Use of any ICT must be appropriate to the College environment

- 2.1 For educational purposes only. The College's computer network, Internet access facilities, computers and other school ICT equipment/devices can be used only for educational purposes appropriate to the College environment. This rule applies to use on or off the College site. If any other use is permitted, the College will inform the user/s concerned. **Students must have teachers permission to access the college ICT facilities and equipment.**
- 2.2 Permitting someone else to use College ICT. Any staff member or student who has a signed use agreement with the College and allows another person who does not have a signed use agreement as per point 1 (above) to use the College ICT, is responsible for that use.
- 2.3 Privately-owned ICT. Use of privately-owned/leased ICT equipment/devices on the College site, or at any College-related activity must be appropriate to the College environment. This includes any images or material present/stored on privately-owned/leased ICT equipment/devices brought onto the College site or to any College-related activity. It also includes the use of mobile phones and cameras. Any queries should be discussed with the ICT Team.
- 2.4 Responsibilities regarding access of inappropriate or illegal material.  
When using College ICT, or privately-owned ICT on the College site or at any College-related activity, users must not:
  - initiate access to inappropriate or illegal material – including but not limited to adult content, online gaming sites, gambling sites, social networking and chat sites such as MySpace and Facebook. The use of Peer-to-Peer software is also prohibited
  - save or distribute such material by copying, storing or printing.

In the event of accidental access of such material, users should:

1. not show others
2. close or minimise the window
3. report the incident
  - Students should report to a teacher immediately
  - Staff should report such access as soon as practicable to the ICT Management Team.

- 2.5 Misuse of ICT. Under no circumstances should ICT be used to facilitate behaviour which is either inappropriate in the College environment or illegal.

Unacceptable use could include acts of a malicious or nuisance nature, invasion of privacy, harassment, bullying, hacking, altering the settings on any ICT device or equipment without authorisation, plagiarism, gaming, impersonation/identity theft, spoofing, gambling, fraud, copyright infringement, or cheating in an examination. Behaviour the College may need to respond to also include the use of websites to facilitate misconduct which puts at risk the safety of the College environment.

- 2.6 Students are not to connect to any external devices e.g. phones, USB modems or other wireless networks while at Parkwood Secondary College. Students found breaching these guidelines will lose access to Parkwood Secondary College's network, and laptops will be reimaged immediately. Deliberate circumvention of school internet filtering, by use of third-party software, external internet connections (such as '3 mobile internet'), or "anonymous proxy" sites will result in the laptop being immediately reimaged, the administrator status of the student will be modified and the student's ability to access the Parkwood Secondary College network will be reviewed.

## 3 Individual password logons (user accounts)

- 3.1 Individual user name and password: If access is required to the College computer network, computers and Internet access using College facilities, it is necessary to obtain a personal user account from the College.
- 3.2 Confidentiality of passwords: It is important to keep passwords confidential and not shared with anyone else.
- 3.3 Access by another person: Users should not allow another person access to any equipment/device logged in under their own user account, unless with special permission from a College staff member (in consultation with a member of the ICT Team). (Any inappropriate or illegal use of the Parkwood Secondary College computer facilities and other College ICT equipment/devices may be traced by means of this login information.)
- 3.4 Appropriate use of email: Those provided with individual, class or group e-mail accounts are expected to use them in a responsible manner and in accordance with this use agreement. This includes ensuring that no electronic communication could cause offence to others or harass or harm them, put the owner of the user account at potential risk, or in any other way be inappropriate in the College environment.

#### **4 Disclosure of personal details**

- 4.1 For personal safety, users should be very careful about revealing personal information about themselves, such as home or email addresses, or any phone numbers including mobile numbers. Nor should such information be passed on about others.

#### **5 Care of ICT equipment/devices**

- 5.1 All College ICT equipment/devices should be cared for in a responsible manner and especially ensuring that laptops or any mobile devices are carried in the bags provided.
- 5.2 Any damage, loss or theft must be reported immediately to the ICT Team. In the event of theft, a police statement must be made as soon as practically possible.
- 5.3 At school, when laptops are not being used or carried by the individual they should be securely stored in a locked locker
- 5.4 At the conclusion of the agreement, or if the student leaves the College before the conclusion of the agreement, the laptop/ICT device must be returned to the College in the same condition as was initially supplied. That is, no stickers, graffiti, white-out, scatches and etchings, cracks, missing keys, discolouration, substances requiring more than light cleaning or any damage beyond normal wear and tear.
- 5.5 Students must not damage or steal any equipment, or try to damage the ICT network. If the damage is deliberate, it will be necessary for the college to inform parent/legal guardian/caregivers who will have responsibility for the cost of the repairs or replacement.

#### **6 Wastage**

- 6.1 All users are expected to practice sensible use to limit wastage of computer resources or bandwidth. This includes unnecessary Internet access, uploads or downloads and printing.

#### **7 Connecting software/hardware**

- 7.1 Users must not attempt to download, install or connect any unauthorised software or hardware onto College ICT equipment, including but not limited to student laptops and iPod Touches or utilise such software/hardware. This includes use of such technologies as Bluetooth, infrared, and wireless, such as mobile broadband internet, and any other similar technologies which may be developed. Any user with a query or a concern about this issue should speak with the ICT Leader.
- 7.2 In a special case where permission has been given by the ICT Leader to connect or install privately-owned equipment/devices or software, it is with the understanding that the College may scan this equipment/device/software at any time thereafter as part of a regular or targeted security check, such as for viruses.

#### **8 Copyright and licensing**

- 8.1 Copyright laws and licensing agreements must be respected. This means no involvement in activities such as illegally copying material in any format, copying software, downloading copyrighted video or audio files, using material accessed on the Internet in order to plagiarise, or illegally using unlicensed products. This means that students are not to have limewire or torrents or any other peer to peer

software on the laptops. It is very clear in the acceptable use agreement which all year 9 to 11 students and a parent have signed. If students are found in breach of these guidelines the laptop will be reimaged immediately. If Peer-to-Peer software, such as Limewire or BitTorrent is found on any laptop/ICT device, the laptop/ICT device will be reimaged.

- 8.2 The College will provide software which is in accordance with the copyright laws and must only be installed on College leased or owned equipment. Once equipment ownership transfers outside of the College it is only legal to have installed the software which originally came with the computer and copyright laws and licensing agreements become the responsibility of the equipment holder.

## **9 Posting material**

- 9.1 All material submitted for publication on the College Internet/Intranet should be appropriate to the College environment.
- 9.2 Such material can be posted only by those given the authority to do so by ICT Team.
- 9.3 The ICT Team, should be consulted regarding links to appropriate websites being placed on the College Internet/Intranet (or browser homepages) to provide quick access to particular sites.
- 9.4 There is only one official website relating to the College with which there should be involvement unless approval has been given by the ICT Team.

## **10 Consequences.**

- 10.1 Depending on the seriousness of a particular breach of the use agreement, an appropriate response will be made by the College in line with the Student Engagement and Wellbeing Policy. Possible responses could include one or more of the following: a discussion with the student, informing parents/legal guardian/caregiver, reimaging of laptop/device, loss of administrator access to laptops/devices, loss of student access to College ICT, taking disciplinary action. If illegal material or activities are involved, it may be necessary for the College to inform the police and/or other government departments.
- 10.2 Where laptops require reimaging due to a breach of this agreement, the laptop/ICT device will not be backed up before reimaging. There will be no opportunity given to the student to back up their work. However, if you wish for work to be backed up, the College ICT Team will back up work for a fee. A fee \$50 will apply on the first occasion and \$100 on every occasion thereafter.
- 10.3 The College reserves the right to confiscate the laptop due to a breach of this agreement.

## **11. Mobile phones.**

Cyber safety rules also apply to mobile phones. Students are not permitted to have a phone on in class time unless this is approved by a staff member. Mobile phones must not be used for involvement with inappropriate material or activities, such as:

- Upsetting or harassing students, staff and other members of the College community even as a 'joke'.
- Inappropriately using text, MMS, email, photographs or film, phone messages, web browsing, images or any other functions.
- During any assessment where such possession or use is specifically prohibited.
- Forwarding private information about another person using Short Message Service (SMS)
- Taking photos, recording sound or video when it is not part of an approved lesson
- Taking photos, recording sound or video when you have not been granted permission by the individual (including teachers)
- Publishing photos, recorded sound or video in any medium (e.g. any online space) or to anyone without appropriate (written) permission from the individual.

## **11 Queries or concerns**

- 11.1 Staff and students should take any queries or concerns regarding technical matters to the Leader.
- 11.2 Queries or concerns regarding other cybersafety issues should be taken to the relevant Sub-School Coordinator.



## **ACCEPTABLE USE AGREEMENT FOR ULTRANET, INTERNET, DIGITAL AND INFORMATION COMMUNICATION TECHNOLOGIES**

### **To the student, and the parent/legal guardian/caregiver**

1. Please read this page carefully, to check you understand your responsibilities under this agreement
2. Sign the appropriate section on this form
3. Detach and return this form to the College office
4. Keep the document for future reference, as well as the copy of this signed page which the College will provide.

### **We understand that Parkwood Secondary College will:**

- Do its best to keep the College cybersafe, by maintaining an effective cybersafety programme. This includes working to restrict access to inappropriate, harmful or illegal material on the Internet or College ICT equipment/devices at College or at College-related activities, and enforcing the cybersafety regulations and responsibilities detailed in use agreements. This also includes protecting the holder of this agreement from external or public sources attempting to access the cybersafe environment within the College
- Keep a copy of this signed use agreement form on file
- Respond appropriately to any breaches of the use agreements
- Provide members of the College community with cybersafety education designed to complement and support the use agreement initiative
- Welcome enquiries from students or parents about cybersafety issues.

---

### **Student's section**

#### **My responsibilities include:**

- I will read this Cybersafety and Acceptable Use Agreement document carefully.
- I will take proper care of my computer and other College ICT equipment/devices and be responsible for its safe storage. I know that if I have been involved in the damage, loss or theft of ICT equipment/devices, my family may have responsibility for the cost of repairs or replacement.
- I will keep this document somewhere safe so I can refer to it in the future.
- I will ask the relevant staff member if I am not sure about anything to do with this agreement.
- I understand that it is my sole responsibility to regularly back up my work to either the College network and/or an external source, such as USB drive. I understand that the College ICT team is not responsible for backing up. In the extreme event of student work requiring backing up by the College, costs will be charged for time taken.
- I will not interfere with any laptop/ICT device that belongs to another student or staff member.
- I understand that allowing anyone other than myself or college appointed ICT Support team to interfere with or use my laptop/ICT device will void the warranty.
- Not revealing my password to anyone except the system administrator or the teacher.
- Not interfering with network security, the data of another user or attempt to log into the network with a user name or password of another student .
- Not bring or download unauthorised programs, including games, to the school or run them on school computers.

#### **When I use digital technology I agree to:**

- Be a safe, responsible and ethical user whenever and wherever I use it and follow all cybersafety rules and instructions (i.e. when using either privately owned or college owned ICT devices/equipment on the college network, Internet access facilities, computers in a college related activity, regardless of its location).
- Support others by being respectful in how I communicate with them and never write or participate in online bullying (this includes forwarding messages and supporting others in harmful, inappropriate or hurtful online behaviour) .
- Avoid any involvement with material or activities which could put at risk my own safety, or the privacy, safety or security of the College or other members of the College community (i.e. by not giving out personal details including full names, telephone numbers, addresses and images).
- Talk to a teacher if I feel uncomfortable or unsafe online or see others participating in unsafe, inappropriate or hurtful online behaviour.
- Seek to understand the terms and conditions of websites and online communities and be aware that content I upload or post is my digital footprint .
- Use the internet for educational purposes and use the equipment properly.
- Use social networking sites for educational purposes and only as directed by teachers.
- Abide by copyright procedures when using content on websites (ask permission to use images, text, audio and video and cite references where necessary) I understand that downloading any music, videos, software etc that I do not own is illegal.
- Think critically about other users' intellectual property and how I use content posted on the internet.

**When I use my mobile phone, iPod or other mobile device I agree to:**

- Keep the device off during class times and only make or answer calls and messages outside of lesson times – except for approved learning purposes
- Protect the privacy of others and never post or forward private information about another person using Short Message Service (SMS)
- Only take photos and record sound or video when it is part of an approved lesson
- Seek permission from individuals involved before taking photos, recording sound or videoing them (including teachers)
- Seek appropriate (written) permission from individuals involved before publishing or sending photos, recorded sound or video to anyone else or to any online space
- Be respectful in the photos I take or video I capture and never use these as a tool for bullying.

**I understand that this Acceptable Use Agreement also applies during school excursions, camps and extra-curricula activities.**

**I have read and understand my responsibilities and agree to abide by this Agreement. I understand that my access to the internet and mobile technology at school will be renegotiated if I do not act responsibly and could potentially lead to serious consequences.**

Name of student: ..... Form: .....  
Student Signature: ..... Date: .....

---

**Section for parent/legal guardian/caregiver**

My responsibilities include:

- I will read this Cybersafety and Acceptable Use Agreement document carefully and discuss it with my son/daughter so we both have a clear understanding of my child's role in the College's work to maintain a cybersafe environment
- I will ensure this use agreement is signed by my child and by me, and returned to the College
- I will encourage my son/daughter to follow the cybersafety rules and instructions
- I will contact the College if there is any aspect of this use agreement I would like to discuss.
- I will ensure that my son/daughter understands and follows their legal copyright responsibilities.
- I understand that allowing others, beyond immediate family, to access or use my son/daughters laptop/ICT device will void the warranty.

**I have read this Cybersafety and Acceptable Use Agreement document and am aware of the College's initiatives to maintain a cybersafe learning environment, including the responsibilities involved.**

Parent/Legal Guardian/Caregiver (Please circle which term is applicable.)

Name: .....

Signature: ..... Date: .....

*For further Support with online issues students can call Kids Helpline on 1800 55 1800. Parents/cares call Parentline 132289 or visit <http://www.cybersmart.gov.au/report.aspx>*